

 <i>An SAE International Group</i>	AEROSPACE INFORMATION REPORT	 AIR6218	
		Issued 2012-09	
Constructing Development Assurance Plan for Integrated Systems			

RATIONALE

This SAE Aerospace Information Report presents a collection of lessons learned for constructing development assurance plans for integrated systems based on past certification programs.

FOREWORD

Integrated aircraft system architectures have flourished in civil aircraft development since the 1990s, and the use of such architectures will likely accelerate in future design practices. To date, the industry standards (and regulatory guidance) on integrated systems have not progressed much further than a firm acknowledgment of the rapid integrated systems growth trend, and a recognition of potential safety risks if development errors are not identified and corrected during the development process. Chapter 4 of the SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, recognizes this issue and states, *"Complex systems and integrated aircraft level functions present greater risk of development error (requirements determination and design errors) and undesirable, unintended effects."* In today's practices, development assurance plans for integrated systems are predominantly based on the tried-and-true concept of separation of responsibilities between various disciplines. This is incongruent with the demands of integrated system architectures. While system separation, fault isolation, or error containment, will continue to be effective risk management practices that must not be compromised or overlooked, a new approach for constructing a development assurance plan for integrated systems is needed to cope with the reality of system design trends.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2012 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

**SAE values your input. To provide feedback
on this Technical Report, please visit
<http://www.sae.org/technical/standards/AIR6218>**

1. SCOPE

This SAE Aerospace Information Report (AIR) supplements ARP4754A by identifying the crucial elements to be considered when constructing the development assurance plans described in Chapter 3 (Development Planning) of ARP4754A for integrated systems. This AIR presents a collection of lessons learned from past certification programs involving integrated systems. This AIR is not guidance for system integration technologies.

2. APPLICABLE DOCUMENTS

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

ARP4754A Guidelines for Development of Civil Aircraft and Systems

Beland, S. and Miller, A., "Assuring a Complex Safety-Critical Systems of Systems," SAE Technical Paper 2007-01-3872, 2007, doi:10.4271/2007-01-3872

3. DEVELOPMENT ASSURANCE PLANNING

Development Assurance involves all of those planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design and implementation have been identified and corrected such that the system satisfies the applicable certification basis. Chapter 3 of ARP4754A provides a general planning process to address development assurance. This general process involves a number of "development planning elements," repeated in Table 1:

TABLE 1 - DEVELOPMENT PLANNING ELEMENTS

Planning Elements	Element Description
Development	Establish the process and methods to be used to provide the framework for the aircraft/system architecture development, integration and implementation.
Safety Program	Establish scope and content of the safety activities related to the development of the aircraft or system.
Requirements Management	Identify and describe how the requirements are captured and managed. Sometimes these elements are included in conjunction with the validation elements.
Validation	Describe how the requirements and assumptions will be shown to be complete and correct.
Implementation Verification	Define the processes and criteria to be applied when showing how the implementation satisfies its requirements.
Configuration Management	Describe the key development related configuration items and how they will be managed.
Process Assurance	Describe the means to assure the practices and procedures to be applied during system development are followed.
Certification	Describe the process and methods that will be used to achieve certification.

The various planning data described in ARP4754A is reproduced graphically in Figure 1 using the traditional development “V” diagram. This graphic conveys a potential for gaps in conventional system development planning to occur (i.e., the white space in between the aircraft plans and the system plans). An integrated system may, therefore, have these same plan disconnects as well as additional system implementation strategy induced short falls.

Although the ARP4754A comprehensively describes a general development process and life cycle, it does not focus on the development assurance activities that are unique to integrated systems. To begin this discussion we need to have a common set of terms. Within this AIR we consider the following:

1. What is an “integrated system”?

In the context of this AIR, an “integrated system” is the set or arrangement of interdependent systems that have complex relationship or connection to provide a given capability. It can be visualized as a system of systems. Integrated systems enable more efficiency and robustness in providing system functions. Shared system resources, especially computers and communication networks, enable the implementation of functions more complex than can be provided by an individual system. However, integrated system architectures can introduce complex mechanisms for cascading failures or other unintended consequences.

2. How is the Development Assurance Plan for Integrated Systems (DAPIS) different from the plan elements shown in Table 1 and graphed in Figure 1?

The planning elements shown in Table 1 and Figure 1 reflect practices commonly associated with the development of stand-alone systems. While the concept they represent is generally applicable to any system arrangement, be it integrated or standalone, DAPIS focuses on the interrelationships between those elements, to help answer lingering concerns that something may be missing or overlooked when integrated systems are developed and certified. Compared to standalone system development, the integrated system plan must contemplate the larger number of multi-dimensional interactions between functions, systems, and the organizations who work on them to minimize the risk of “missing something important.” This AIR provides a “hands-on” set of elements based on lessons learned from past certification programs.

Because a plan is tailored to the needs of the individual project, the elements discussed in Section 4 are not intended to be a general “template”. Rather, they provide insights on issues that experience has shown may not always be obvious (i.e., missing) when the development assurance activities of ARP4754A are planned or executed.

4. DEVELOPMENT ASSURANCE PLANNING FOR INTEGRATED SYSTEMS (DAPIS)

The classic planning considerations prescribed in ARP4754A provide for nominal integration of systems with considerations for the physical interfaces between electrical systems, interfaces between electrical systems and mechanical systems, or logical interfaces between hardware and software. These considerations may not be enough to assure the development of integrated systems.

The planning elements for integrated systems should also be considered when executing the planning process described in ARP4754A. DAPIS effects on the overall planning process should cover some or all of the following: design, test, manufacturing, maintenance, make allowances for follow-on product improvement. The following integrated systems effects on the ARP4754A plans should be contemplated. [Note: As the following information is a collection of “lessons learned,” readers should assess them for applicability to their projects and the equivalency of their existing methods and tools.]

Figure 2 presents the additional planning and implementation relationships for integrated systems. The magenta highlighted integration plans gain importance when the development objective is an integrated system. The mechanisms for interface control also increase the interactions between activities and enhance communication for the integrated system.

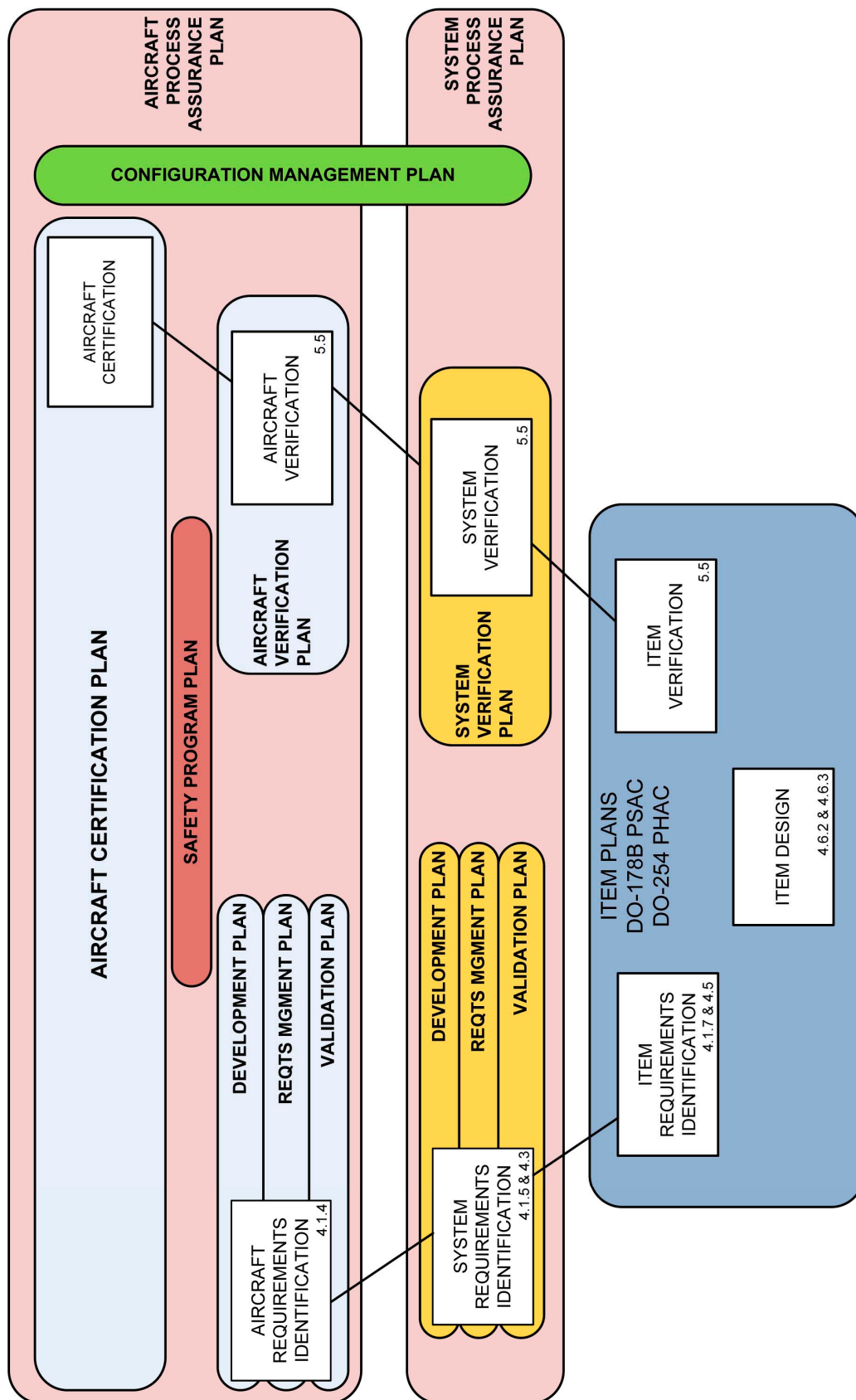


FIGURE 1 - ARP4754A PLANNING RELATIONSHIPS

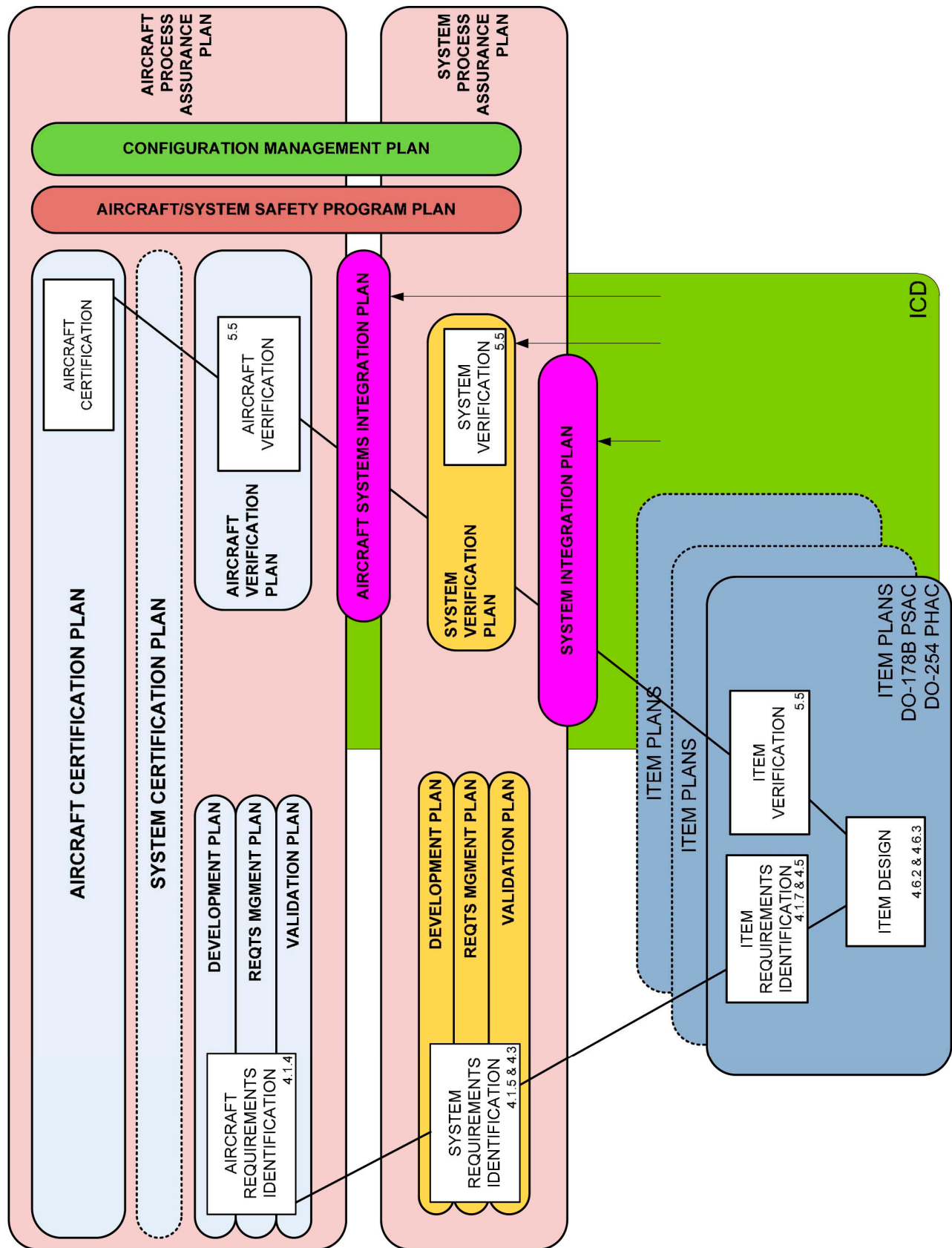


FIGURE 2 - DAPIS PLANNING RELATIONSHIP

4.1 DAPIS Effects on Aircraft Certification Plans

- It is crucial that the system-level plans are congruent with each other and with the aircraft-level plan. The OEM should conduct oversight to ensure process assurance, and the objectives of the aircraft-level plan are met by the system-level plans.
- Aircraft-level plans should be developed early in the development, before the system-level plans are completed.

4.1.1 Certification and Safety Issue Identification

- Develop a communication plan (e.g., organization and schedule for technical panels discussion with certification authorities). A technical panel dedicated to aircraft-level safety is recommended for a new aircraft program. See also the discussion on “Master documents” below.
- Communicate the “design for safety” approaches within a developer’s organization. Integrated system development can no longer rely on stovepipe practices where safety activities are separate from the design activities. It is a collaborative, not independent effort, between Safety and Design organizations. Appendix B of ARP4754A provides guidelines for the creation of a Safety Program Plan which can be used to develop the interface between the design and safety organizations.
- The safety assessments need to contemplate the effects of having multiple functional failures (e.g., loss, degradation or erroneous operation) that could result from a single shared resource failure. Although an individual functional failure is not so severe, in combinations they may have a more severe hazard classification than the effects of any one of the functions taken alone.

4.2 DAPIS Effects on Safety Program Plans

4.2.1 “Master” Documents

The use of “master” documents to capture the development process to be applied across all systems and their interfaces is recommended. This master document serves as a reference point for anyone working on the program to use as an authoritative source of common information. This master document should contain (or have pointers to) the following types of information:

- The common set of data related to the intended operations of the product (for example, average flight profile, probability values of specific failures or external events, specific criteria that are not apparent in the regulatory guidance, etc.). This set of data is used as a baseline for all safety analyses performed on the product.
- The overarching safety analysis methods that clarify, or expand on, aspects of selected regulations to ensure consistency of understanding of such regulations, and compliance determination between interfacing systems.
- Completion criteria for the development assurance activities, especially completion criteria for the validation and verification activities. These criteria, or at least a framework thereof, should be developed and presented to the certification authorities as early as possible in the development life cycle.

It is recommended that “master documents” be agreed to by all influencing parties at the beginning of the program.

4.3 DAPIS Effects on Development Plans (for aircraft and system-level process assurance)

4.3.1 Organizational Interaction Management

The responsibilities, capabilities, work statements for each activity should be defined across organizational and programmatic execution boundaries, for example, interactions between the OEM and the suppliers, or between the organizations internal to the OEM. This establishes the roles and responsibility expectations for system integrators, suppliers, etc. for validation, verification, process assurance, configuration management and problem reporting.

4.3.2 Integrated System Boundary Definition

A definition of what the integrated system will encompass should be defined. The integrated system boundary may encompass:

- Aircraft and system functions.
- Aircraft and system architectures, and their interdependencies.
- Man-machine interfaces, especially a strategy for multiple (and potentially simultaneous) alerting functions. While integrated systems can ease flight crew workload, a failure in an integrated system can generate multiple alerts (e.g., through cascading effects) and may complicate flight crew's ability to isolate or prioritize corrective actions.
- Shared resource capabilities and capacities.
- Criteria for selecting which functions are to be integrated (e.g., use the shared resource), and which should stand alone. This involves an analysis of the criticalities of the functions, leading to the identification of the potential needs for more rigorous controls of selected functions or design parameters.

4.3.3 System Interface Management

The following system interface constructs are recommended for integrated systems:

- Develop and manage an "aircraft data dictionary" and interface requirements to accommodate correct demarcation of functional boundaries and to avoid inadvertent use of data or retention of orphaned data. The data dictionary and interface requirements may be combined in the same data set; but if kept separate, traceability between them should be maintained.
- There should be a "resource assurance analysis" to confirm that functions of one development assurance level (DAL) are not adversely affected by functions of a lesser DAL, and where it does, that there is a documented rationale on why that approach is acceptable. In an integrated environment, a single data source is efficient, but the development assurance level of a data source may not globally satisfy all users, because the source of the parameters may not have the DAL required by the users. This is a balancing act, because having to develop separate data sources to meet the development assurance requirements of specific users reduces the value of "integration." A data integrity analysis may be included in this analysis.
- Ensure the functionality of one system in the integrated architecture does not depend on the internal details of another system unless the interdependencies are captured in the requirements of both systems.
- Ensure the functionality of one item in a system does not depend on the internal details of another item unless the interdependencies are captured in the requirements of both items.
- Procedures for correction/recovery in the event of interface errors.

4.4 DAPIS Effects on Item Plans

Although an item (e.g., software, hardware) is a part of an integrated system, so far, we have not identified any lessons learned in this area. We welcome reader inputs for this section, to be added in a future update of this document.

4.5 DAPIS Effects on Validation and Verification Plans (for aircraft and system levels)

4.5.1 Validation and Verification Methods

It is important that the DAPIS contain material addressing the following aircraft and systems validation and verification activities:

- Validation Methods - Identify critical sub-processes at the system level, such as requirement capture and management activities described in ARP4754A to highlight the links between the integrated systems/functions.
- In-Service Experience - Lessons learned from the field is usually a method to validate requirements, assumptions, or system architectures. It is recommended that there be a planned activity to capture and apply in-service experience in the development assurance process.

As an example, specific attention should be given to monitoring functions. In service experience related to inadequate behaviors of monitor functions pointed to the need for better verification of monitor function coverage. This verification should be systematic for digital systems and should consider the monitoring function behavior when the monitored signal is stuck at fix values and when it is affected by oscillatory, sudden and large impulses, or sawtooth signals. The frequencies of the signals should also be considered in the monitoring function behavior especially when these frequencies are close or identical to the computation cycle of the monitoring function. A systematic design study on the monitor coverage as well as the weakness in this coverage should be systematically planned for digital systems to assure that they will perform failure detection as intended.

- Architecture validation techniques, such as the Preliminary Aircraft Safety Assessment (PASA) and Preliminary System Safety Assessment (PSSA) need to highlight inter-relationship considerations. Ensure the safety analyses keep up with the changes to the aircraft and systems during the development.
- Specific assurance activities that ARP4754A may not cover in sufficient detail (for example considerations for setting up an integrated test rig) should be described (e.g., stating "assured to FDAL X" may be too vague at the aircraft/system level).
- Systematic approaches to Common Causes Analyses and/or generic error assessment with synergistic organized approaches to mitigating common mode or cascading failures and/or generic errors in critical systems should be addressed.
- A functional coverage assessment (one which spans all systems that support a given function) should be accomplished.
- Planners often assume one-time-fly-through success and don't allow time to react to issues.
- Bench test procedures should be defined. Bench configuration management alone is not sufficient for Validation and Verification purposes.
- Because currently there is no regulatory guidance for determining credits for using bench testing for V&V, discuss test plans and intent for taking credits of bench tests with the certification authorities.

- Safety reviews should be conducted in a manner that emphasizes the interaction between the functions, the systems, and items as well as the technical content of the safety assessment/analyses (FHA, PASA/PSSA/SSA/ASA, CMA, PRA, etc.). The reviews should evaluate the application and effectiveness of the Validation/Verification processes, the associated results, and assure transition criteria are met. Appendix B of ARP4754A provides guidelines for the creation of a Safety Program Plan which can be used to identify these types of review.

4.6 DAPIS Effects on Configuration Management and Process Assurance Plans

- Be aware of disconnected problem reporting systems between airplane systems, between systems and items, or between integrator and suppliers. Provide the means for either one single PR system or for the various PR systems to be linked to support traceability and full visibility to the integrators while protecting individual supplier companies' proprietary data where needed.
- Reverse engineering an assurance process to catch up with lack of evidence that systemic assurance activities were performed will not provide the confidence that an assurance process is effective.
- Deviation Management
 - Define provision for how the plan will be enforced (i.e., process assurance).
 - Define a process to handle deviations from completion criteria.
 - Define what the outputs are going to be (i.e., what are the artifacts to show compliance to the plan?).
 - Because designs can and do change after implementation or late in the program, there should be a mechanism described for and be traceable to:
 - change impact assessment
 - regression analysis

4.7 Organization Support for Integrated System Development

- As the use of ARP4754A involves a new learning curve and organizational commitment, a job aid for DERs/ARs on the use of ARP4754A may provide them the authority they need within their organizations to promote the development of a DAPIS, and consistent application of the ARP4754A.
- In light of the trend toward "self-certification" the aircraft/system developer's organization needs a process to track and communicate when completion criteria have or have not been met.

4.8 Things to Consider

- Be aware of incorrect assumptions for taking TSO credits. In electronic hardware and software qualifications, meeting TSO requirements alone for the products is insufficient when installed on the aircraft.
- PDR and CDR should evaluate interface and integration between functions, not just the functions in and of themselves
- Certification authorities may focus on different aspects, for example, integration versus development assurance. A harmonized description of what it takes to be finished should be developed.

4.9 DAPIS Summary and Conclusion

This AIR captures a number of lessons learned from past certification programs that involved integrated systems. The complexity of integrated systems raises a demand for an integrated approach as early as the planning phase of the development assurance activity. As the aerospace industry gains experience using ARP4754A, more lessons learned can be expected in the future and this AIR may be revised to capture new lessons learned as the need arises.

5. NOTES

- 5.1 A change bar (I) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY SAE COMMITTEE S-18, AIRCRAFT & SYSTEMS DEVELOPMENT AND SAFETY ASSESSMENT